CASO DE SOTO PRIETO: APERTURA A UNA NUEVA LEGISLACIÓN EN DELITOS DE CARÁCTER INFORMÁTICO

Cristhian Daniel Torres Villamarín*
Universidad Católica de Colombia

Resumen

Con el avance tecnológico mundial los delitos evolucionan, siendo por esto necesaria la constante evaluación de los delitos sancionados por la legislación penal en un país, es por esto que el presente artículo pretende, con base en el caso Soto Prieto, profundizar en los delitos informáticos, tipificados en el Código Penal ley 599/ 2000, Titulo VII de la protección de la información y de los datos, Capítulo I de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; y en el Capítulo II de los atentados informáticos y otras actuaciones. Enfocándonos de este modo en el avance tecnológico, estableciendo conceptos claros, las principales características, cuáles son las normas que regulan tanto nacional como internacionalmente los delitos informáticos, con el fin de establecer la eficacia de los procedimientos y normas creadas para dar respuesta inmediata a los casos que representan un riesgo no solo respecto a la seguridad informática sino también los delitos que de allí se derivan.

Palabras Claves: Delitos informáticos, Legislación, Cibercriminales, tipicidad del delito informático, Derecho penal.

Abstract

With the global technological advance, crimes evolve, that is why the constant evaluation of crimes sanctioned by criminal legislation in a given country is necessary, and that is why this article intends, based on the Soto Prieto case, a deep analysis of computer crimes, typified in the Criminal Code, Law 599/2000, Title VII on the protection of information and data, Chapter I on the attacks on confidentiality, integrity and availability of data and computer

*Estudiante de derecho Universidad Católica de Colombia; CC. 1.020.790.813 de Bogotá; Cód. 2109907; Email cdtorres07@ucatolica.edu.co. Articulo reflexivo para optar al título de abogado. Director: Dr. Jorge Restrepo Fontalvo, profesor titular en la cátedra de Derecho penal.

systems; and in Chapter II on the computer attacks and other actions. Focusing on technological advancement, establishing clear concepts, and it is main characteristics, and also analyzing the norms local and international, that regulate computer crimes, in order to establish the effectiveness of the procedures and norms created to immediately respond to cases which represent a risk, not only with regard to computer security but also the crimes that derive from it.

Keywords: Computer crimes, Legislation, Cybercriminals, type of computer crime, criminal law.

Sumario

Introducción

Ante el desarrollo de los sistemas informáticos en el mundo y su implicación en grades aspectos de la

> vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica delitos informáticos, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática (Ojeda Perez J. E., Rincon Rodriguez, Arias Flores, & Daza Martinez , 2010, pág. 43).

El trabajo consiste en plasmar los conocimientos que se adquieren al realizar una investigación y análisis, con el fin de conocer a fondo "la variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones." (Avendaño, 2017, pág. 5).

El objetivo fundamental del presente trabajo es adquirir elementos de juicio claros sobre los delitos informáticos y su contexto, partiendo del caso Soto Prieto, el cual establece las bases para la normatividad aplicable a este fenómeno delictivo; en consecuencia señalar qué son los delitos informáticos, cuáles son las principales características, cuáles son las normas que los regulan, normas de carácter mundial acerca del tema, legislación y jurisprudencia colombiana, medios de control y finalmente emitir conclusiones respecto de la efectividad de las normas y la debilidad de las instituciones con atención a los delitos señalados. Así mismo es necesario hablar acerca del tema central del trabajo, que no es más que la eficacia de la legislación actual respeto a los delitos informáticos como un grupo genéricos de delitos, puesto que en la actualidad la sociedad se mantiene en constante cambio, por lo cual los medios de comunicación masiva encuentran importancia dentro de la actualidad, siendo el internet y la facilidad que éste nos brinda en tareas cotidianas, como el pago de recibos, transacciones, búsqueda de cuentas bancarias, estabilidad financiera de determinado sujeto, entre otro tipo de información no solo económica sino a nivel personal; siendo de este modo el internet una fuente inagotable de información.

Respecto a lo anterior debemos tener en cuenta que el internet no solo nos brinda información para mejorar nuestra manera de investigar y conocer las cosas, esto nos hace entender que cualquiera puede hacer uso de la información que consiga por medios electrónicos encontrándonos en la necesidad de actuar frente a los diferentes medios y mecanismos por los cuales se pueden cometer actos en contra de la ley. De acuerdo con Computer Forensic (s.f.) los delitos informáticos se definen como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" esto quiere decir, que estos delitos son aquellos cuyas actividades ilícitas se cometen, entre, otros:

- Fraudes cometidos mediante manipulación de computadoras.

- Manipulación de datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

El economista Roberto Soto Prieto, quien ejerció funciones como secretario General del ministerio de Desarrollo, viceministro de cartera en 1976 fue acusado como el cerebro de un robo de 13.5 millones de dólares de una cuenta del gobierno colombiano del Chase Manhattan Bank. Con base en la acusación presentada en su contra se profundizará en los delitos informáticos, tipificados en el Código Penal ley 599/ 2000, Titulo VII de la protección de la información y de los datos, Capítulo I de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; y en el Capítulo II de los atentados informáticos y otras actuaciones. Enfocándonos en los conceptos principales emitidos por diferentes doctrinantes, así mismo establecer qué son los delitos informáticos, cuáles son las principales características, cuáles son las normas que los regulan, las normas de carácter mundial acerca del tema, legislación y jurisprudencia colombiana, medios de control y finalmente conclusiones frete al caso.

1. Contextualización: Caso Soto Prieto

Con la intención de sentar las bases para el presente artículo, se establecerá un análisis histórico y descriptivo del caso de Roberto Soto Prieto, el cual constituyó el motivo principal para la creación de normas, suficientes o no, para la protección de la información y transacción realizadas por medios electrónicos, los cuales hoy en día conforman una fuerza económica e informativa suficiente que evoluciona a grandes pasos, de acuerdo con las necesidades fluctuantes de los mercados y comercios. Para esto, se profundizará en las acciones ejecutadas para lograr extraer la cuantiosa suma de dinero señalada por medio de artificios y mecanismos que para la época del mismo eran desconocidos, así mismo se realizará un análisis de la sentencia por medio de la cual se condena al señor Roberto Soto Prieto por los delitos cometidos.

De acuerdo con la reseña de la vida y obra, más bien del fraude ejecutado contra el Estado colombiano realizada por Hillon Vega (2000) quien cita el artículo del periódico El tiempo ¿Quiénes son los responsables? Establece:

> Roberto Soto Prieto fue un economista, nacido en Bogotá el 6 de diciembre De 1944. Hijo de Jaime Soto y Sofía Prieto. Casado con María Cebollero de Soto. Tiene tres hijos, Mafalda Carolina, María José y Mónica Claudia. Se graduó en la Universidad de Friburgo (Suiza). Se especializó en comercio exterior, en el Centro de Comercio Internacional de Undadgart. Fue jefe de la sección de Comercio Exterior del Ministerio de Relaciones Exteriores, subsecretario asistente y subsecretario de Asuntos Económicos del Ministerio de Relaciones Exteriores y secretario general del Ministerio de Desarrollo. Habla alemán, inglés, francés, además del español. Ha sido profesor en el Instituto Colombiano de Estudios Internacionales del Ministerio de Relaciones Exteriores, conferencista de la Sociedad Colombiana de Economistas y de la Escuela Superior de Guerra. Fue gerente general de la Empresa Latinoamericana de Industria y Comercio — Licsa - dedicada a la explotación de maderas. (El Tiempo, 1984).

Soto Prieto, luego de las investigaciones oficiales que se realizaron alrededor del fraude, fue sindicado como el cabecilla de toda la operación de hurto de 13.5 millones de dólares, provenientes de un contrato de empréstito celebrado entre la república de Colombia como prestatario y el Chase Manhattan Bank con el fin de dotar de equipos al ministerio de Defensa Nacional y la refinanciación de una porción de la deuda pública. Esto ratificado tanto en los testimonios como en las consideraciones de la sentencia proferida por el Juzgado 17 Superior de Bogotá del 4 de agosto de 1886 cuyo magistrado ponente, Doctor Antonio Medina Izquierdo, providencia en la cual se estableció:

> El Gobierno Nacional celebró un empréstito el 10 de mayo de 1982, por la suma de US$ 47.225.317,94, con destino a las FF.AA., siendo Agente el Chase Manhattan de Londres; en dicho contrato se crearon los mecanismos necesarios para la utilización de los fondos y se estableció una subcuenta sobre la cual se efectuaban los desembolsos. El 10 de mayo de 1983, fecha límite para realizar los desembolsos, existía un saldo de US$13.727,33, que fue transferido de la cuenta principal a la subcuenta para ser utilizados posteriormente. El 12 de mayo, apareció un retiro por la suma de US$ 13.5 millones, solicitada la reconfirmación del estado de la cuenta, el Banco respondió acompañando una copia del télex en el cual, supuestamente, se había

enviado u ordenado el traslado de aquella suma a la cuenta No.66711957 del Banco Morgan Guaranty de Nueva York. Dicho télex aparecía colocado en una máquina del Banco de la República, No.45407. Por los anteriores hechos, fueron residenciados en juicio criminal de trámite ordinario:

Roberto Soto Prieto, hijo de Jaime y Sofía, natural de Bogotá, economista, portador de la C. De C. No. 9.067.157 de Bogotá.

Robert Henry Russell, ciudadano norteamericano, al parecer residente en el 15002 Howland, Houston, Texas, Estados Unidos, nacido el 9 de marzo de 1932, comerciante.

Antonio Cebollero y Campo, hijo de Antonio y Carmen, natural de Burgos −España−, economista, casado con Margarita Cebollero Loy, residente en la Avenida de El Lago con calle Petecuy, número 37 de Cali, portador de la C. de Extranjería No. 193689 de Bogotá."[…] "En el desarrollo de la investigación, se estableció que los US$ 13.5 millones, fueron a la cuenta No.18061 del Banco Hapoalim −Zurich−en donde figuró la orden del cuentacorrentista −Russell− por ventanilla y al señor Alberto Lara González, la suma de US$ 13.331.000 quien se identificó con el pasaporte colombiano No. AA 488312, dicha orden se emitió en mayo 16/83, luego se corrigió −mayo 23−en donde se dieron nuevas instrucciones −US$ 100.000 a Houston, US$ 568.500 a otra cuenta y el resto al Banco Leumi de Panamá−." […] "Testimonio. Fueron recibidos los de los siguientes declarantes: ... Jorge Serpa Erazo, Director de Crédito Público del Ministerio de Hacienda, Leonor Montoya Álvarez, Viceministra..."[…]

En principio, se desconocía procesalmente la participación de este encausado en la comisión de los hechos averiguados y esclarecidos a través de este proceso. Su relación con los punibles se desprendió cuando el investigador Dr. Jaime Hernández Salazar, luego de regresar de HOUSTON, TEXAS, estableció que Soto Prieto estaba íntimamente vinculado con el señor Roberto Henry Russell, titular de una cuenta en el Morgan Guaranty de Nueva York, en donde habían sido trasladados los 13.5 millones de dólares, en cumplimiento de instrucciones impartidas y contenidas en los

> télex apócrifos que obran en el proceso." […] "Está plenamente demostrado a lo largo del extenso expediente, que se trata de una persona que tiene como profesión economista, y que además logró desempeñar altos cargos en la administración pública, entre ellos el de haber sido Secretario General del Ministerio de Desarrollo Económico, también desempeñó funciones diplomáticas (Fles. 435 y 436 C.O. No. 4), lo cual se acreditó con fotocopia auténtica del pasaporte de tal naturaleza, enviado por el Ministerio de Relaciones Exteriores, y para la época en que sucedieron los hechos, o sea para el mes de mayo de 1983, representaba en Colombia al Banco BHF de Alemania, en donde había celebrado en nombre del mismo, un contrato con la República de Colombia, y en el cual para su cumplimiento se utilizó un sistema de subcuenta, similar al previsto en el empréstito de los 13.5 millones de dólares. Como instituciones, fundó la empresa privada Licsa, en donde casualmente había instalado dos máquinas télex. Además habla perfectamente el idioma alemán y el inglés; de acuerdo a sus relaciones comerciales y sociales, se infiere claramente que vivía en contacto permanente con personas nacionales y extranjeras con amplios conocimientos de operaciones y transacciones mercantiles, especialmente bancarias. (Garcia Vasquez, 2012).

A pesar de que se encuentra clara la culpabilidad y autoría del economista, vale la pena resaltar el método por medio del cual se procedió a realizar el fraude, puesto que para ese entonces y por cuestiones del principio de legalidad, el cual, de acuerdo a Hernán Alejandro Olano citado en (Bolivar Mesa, 2018), "supone que todas las autoridades de un Estado, en sus acciones, están sometidas a la ley", impedía la aplicación de tipos penales tales como el hurto por medio informáticos tipificado en la actualidad en el artículo 269I del código penal. El día 12 de mayo a las 2:40 a.m., hora y fecha de Londres-Inglaterra, Una máquina télex es receptora de un mensaje que provenía del Banco de la República de Colombia, cuyo contenido es el siguiente:

> 2765 BOGOTA, MAYO 11 DE 19...
> CHASE MANHATTAN BANK
> LONDRES
> REF: REPUBLICA DE COLOMBIA US DLR 47.225.317

LOAN FROM 10.5.82
ATENTAMENTE CON CARGO A LOS FONDOS **DEL PRESTAMO DE LA SUBCUENTA**
DEFFFFSDSFD
45407 BRB“STF AEDIT125/T23 120352 TESTA028 120352
TX1: 45407 BRBG CO
PRI TLX016 120240 AEDIT116 120351...NO SOM
45407 BRBG CO
G CO...
.. EOT
NNNN” Negrilla fuera del texto original (Holguin, 1991, pág. 29).

No obstante el télex enviado contenía errores que requirieron por tanto el envío de un nuevo télex unos cuantos minutos posteriores al envío del primero corrigiendo la cifra solicitada y el lugar de depósito de la misma de la siguiente manera:

PRI TLX017 120249 AEDIT117 120352 ...NO SOM
PLA
PLS AVOID DUPLICATION
PLS AVIOD DUPLICATION
2765 BOGOTA MAYO 11 DE 19...
CHASE MANHATTAN BANK
LONDRES
REF: REPUBLICA DE COLOMBIA US DLR 47.225.317,49
LOANFROM 10.5.82
ATENTAMENTE CON CARGO A LOS FONDOS DE LA SUBCUENTA DEL PRESTAMO EN REFERENBCIA, ENTRE LA REPUBLICA DE COLOMBIA Y UN GRUPO DE BANCOS, CON EL CHASE MANHATTAN BANK COMO AGENTE, LES RUEGO GIRAR, VALOR MAYO 12 DE 19... **LA SUMA DE 13.500.000(TRECE MILLONES DE DOLARES USA)** AL MORGAN GUARANTEE BANK NEW YORK,

CUENTA 66711957 REPUBLICA DE COLOMBIA, PRE- SUPUESTO REFERENCIA 18061 FAVOR AVISARNOS CONFIRMACION GIRO AL TELEX 45407 BRBG CO C/O BANCO DE LA REPUBLICA DE COLOMBIA

CORDIALMENTE

JORGE SERPA ERAZO

DIRECTOR GENERAL DE CREDITO PÚBLICO

MINISTERIO DE HACIENDA Y CREDITO PÚBLICO

20:48

45407 BRBG CO...

... EOT

NNNN

ABCDEFABCDEF**.** Negrilla fuera del texto original (Holguin, 1991, pág. 30)**.** Sin embargo, se comenten nuevos errores existiendo en esta oportunidad un desfase de quinientos mil dólares entre el valor escrito con letras y el valor escrito con números, por tanto se envía un nuevo télex para completar así el millonario fraude.

PRI TLX026 120507 AEDIT165 20527...NO SOM

2766 BOGOTA MAYO 11 DE 19...

REF: REPUBLICA DE COLOMBIA US DLR 47.225.317,49

LOAN FROM 10.5.82

NOS REFERIMOS A NUESTRO ANTERIOR CON LA REFERENCIA ARRIBA MENCIONADA Y CORRE-GIMOS: DEBVE DECIR 13.500.000.00 -TRECE

MILLONES QUINIENTOS MILDE DOLARES USA-,

CORDIALDEMENTE

JORGE SERPA ERAZO DIRECTOR GENERAL DE

CREDITO PUBVLICO

MINISTERIOS DE HACIENDA Y CREDITO PÚBLICO

45407 BRBG CO...

...EOT

NNN

BCDEFABCDEF. Negrilla fuera del texto original (Holguin, 1991, pág. 31).

Por medio de los télex mencionados, Roberto Soto Prieto junto a sus colaboradores realizaron uno de los fraudes electrónicos más grandes en la historia de Colombia; estos sujetos, gracias al avance de la tecnología, lograron interceptar una línea de télex del banco de la república, y posteriormente enviar la orden al banco Chase Manhattan de Londres de transferir esta gran suma de dinero a una cuenta personal del señor Robert Henry Russell, cuenta desde la cual se comenzarían a mover los dineros en un intento de extraviarlos sin que quedara rastro de estos no siendo hasta el "12 de octubre de 1983, cuando pidieron el extracto y encontraron que la República de Colombia, en una cuenta de 15 millones, tenía un saldo apenas de 1.5 millones." (Caceres Corrales, 2013, pág. 96) a pesar del conocimiento por parte de los entes sobre la culpabilidad de los autores y coautores del hurto informático este quedó en la sombra, dada la necesidad de los dineros y la necesidad de demostrar que la corrupción en las entidades encargadas era inexistente, así "el gobierno optó por cobijar con la impunidad a su burocracia con el confeso fin de recuperar el dinero, no por parte de los delincuentes sino de los bancos que habían sido descuidados en la operación de las transferencias." (Caceres Corrales, 2013, pág. 97). Siendo entonces tal y como lo describe el mismo autor "Un fraude exitoso unido a un culposo encubrimiento oficial igualmente eficaz" (ibídem, pag.100).

2. Antecedentes a los delitos informáticos

Con la aparición de la primera computadora en la década de los 50, se dio inicio a una serie de nuevas tecnologías, usadas en el campo estratégico de la guerra. De este modo, la explotación de la máquina, como tal, estaba ligada a un campo en específico por lo cual el aprovechamiento no implicaba el manejo de información económica de las personas que ingresaban a la misma, sin embargo de acuerdo a lo establecido por Manjarrez Bolaños & Jiménez Tarriba (2012) que no

> Fue hasta los años 60 cuando aparecieron, principalmente en Alemania y en Estados Unidos, los primeros artículos y publicaciones sobre casos conocidos de abusos

> informáticos (manipulaciones de ordenadores, de sabotaje de programas informáticos, de espionaje de datos informáticos, e incluso de uso ilegal de sistemas informáticos), esto es, manifestaciones del nuevo fenómeno de la criminalidad informática. (pág. 73).

Entendiendo entonces que el desarrollo de los delitos informáticos está ligado al crecimiento tecnológico, por lo cual tal y como lo determina Rinaldi (2017)

> el primer caso en el que alguien cometió un delito a través de una red de ordenadores, es imposible saberlo. Lo que es posible saber es el primer gran ataque a una red digital y luego usar eso como punto de referencia en la evolución de los delitos cibernéticos.

Siendo entonces el primer caso de delitos informáticos o delitos por medio informáticos encontrado y estudiado

> el caso de Draper Jhon, en Septiembre de 1970, también conocido como el Captain Curnch, descubre que los obsequios ofrecidos en la caja de cereal Captain Curnch duplica perfectamente la frecuencia del tono 2600 hz de una línea de WATS permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT & T. (Manjarrez Bolaños & Jiménez Tarriba, 2012, págs. 73-74).

Del hallazgo de este primer caso se desprendieron todos los incidentes posibles que implicaban el uso de elementos electrónicos. Allí es cuando surge el llamado derecho informático comprendido como

> la acumulación y uso indebido de los llamados datos personales, con el posible conflicto de este hecho y el derecho de intimidad o privacidad. También los contratos de equipamiento informático y la protección a los autores de los programas de computación, en cuanto a los derechos morales y de explotación de su obra; aparecen entre estas primeras inquietudes desarrolladas y ampliadas rápidamente en los sucesivos años. (Ibídem, Pág. 74).

La informática jurídica nace a raíz de la investigación científica de los conflictos jurídicos. La informática jurídica, que es el tratamiento lógico y razonable de la información jurídica, y el derecho de la informática, que engloba los problemas jurídicos producidos por la

informática misma. Finalmente, el termino delito informático surge en el año 90, una vez se fue expandiendo internet por Norteamérica, fundándose por esto el grupo G8, con el fin de estudiar los problemas que surgen por la criminalidad propiciados por internet o que migraron al mismo. Es entonces a partir del año 2000 con el apogeo de las redes sociales y la ratificación de los medios informáticos como influyentes en los atentados perpetuados en el año 2001 que se comprendió la necesidad de establecer una serie de normas que implicaran el impedimento a la industria criminal global para perpetuar dichos delitos. Creando la necesidad de una nueva legislación sobre los siguientes temas:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos relacionados con las computadoras falsificación y fraude.
- Delitos relacionados con el contenido pornografía.
- Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- Responsabilidades secundarias y sanciones cooperación delictiva, responsabilidad empresarial.

3. Aproximación a los delitos informáticos

A continuación se desarrollará todo lo concerniente a la teoría del caso, explicando de este modo qué es un delito informático, tipificación de delito, el modus operandi en este tipo de delitos con el fin de entrar en materia frente a la suficiencia y eficacia de la legislación actual en los casos tales como la defraudación, intromisión o hurto a través de medio informáticos.

¿Qué es un delito informático?

A pesar de que puede ser fácil precisar este tipo de acciones, no se tiene claro una definición concisa del tema dado que engloba las acciones de la cibercriminalidad alrededor del mundo. Por consiguiente, se citarán ciertas definiciones emitidas por autores interesados en el estudio de los crímenes cometidos a consecuencia del desarrollo de nuevas tecnologías y del avance global.

María de la Luz Lima (1984) expresa textualmente, en su libro Delitos Electrónicos, la siguiente definición:

> el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea cómo método, medio o fin. (Pág.100).

Esta autora describe este tipo de delitos como las acciones encaminadas al daño, aprovechamiento propio o ajeno usado como medio, método o fin cualquier instrumento que aborde la globalización de las nuevas tecnologías.

Sin embargo, Luis Orlando Paloma Parra, en el libro Delitos Informáticos da una definición un poco más completa de lo que se puede comprender como delito informático

> el delito informático, o como se conoce en algunas partes del mundo, es una infracción electrónica, que mediante operaciones ilícitas realizadas por medio de la red o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet, son ejecutadas por la ciberdelincuencia. Estas clases que define un delito informático son aún mayores y complicadas y pueden contener delitos tradicionales como hurto, estafas, etcétera, en los cuales los protagonistas principales son los ordenadores y los tejidos virtuales que han sido utilizados (Paolma Parra, 2012).

Así mismo determinan Loredo Gonzalez & Ramirez Granados (2013) que el "Delito informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país"(Pág. 45), no obstante esta definición implica la necesidad de establecer el concepto de sistema informático, el cual de acuerdo con el convenio sobre la Ciberdelincuencia de Budapest es entendido como "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa" (Consejo de Europa, 2001)

abarcando de este modo todo mecanismo por medio del cual se puedan ejecutar programas que implique el manejo y/o manipulación de datos.

Finalmente, el doctrinante colombiano Henry William Torres Torres define al delito informático como

> toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software al que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como infracción informática (Torres Torres, 2002, Pág. 58).

De modo que, a fin de concluir, los delitos informáticos son todas aquellas conductas con posibilidad de ser sancionada por el derecho penal, debido al uso inadecuado de información y/o métodos informáticos o tecnológicos empleados para esto, sin importar que estos sean usados como medio, método o fin, Esto en perjuicio de la libertad de las personas (naturales o jurídicas), su patrimonio, derecho a la intimidad, al buen nombre entre otros.

En el párrafo anterior se estableció las formas por medio de las cuales se puede por acción u omisión incurrir en la conducta punible ya mencionada, estos se explican de la siguiente manera:

- Como método: en este caso se usan técnicas de carácter electrónico para lograr el ilícito.
- Como medio: son acciones criminales en donde se usan instrumentos de carácter tecnológico (computador, Tablet) para lograr el fin.
- Como fin: esto quiere decir que el delito se dirige contra de la entidad física del objeto es decir contra el material electrónico (Lima, 1984).

> Dicho de otra manera, en este contexto, se puede decir que delito informático es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien jurídico que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho. (Rodríguez Arbelaes, 2011).

De acuerdo a lo anterior, es adecuado mencionar las formas de ejecución de dichos delitos en Colombia, según lo investigado por Torres Estepa, Lopez Sanabria, & Sarmiento Avella (s.f) las formas de ejecución específicamente relacionadas por las autoridades en la materia son:

> Fraudes cometidos mediante manipulación de computadores entre estos se encuentra la manipulación de datos de entrada y de salida y la manipulación de programas; se trata es de colocar datos falsos en un sistema u obtener los datos del sistema en forma ilegal.
>
> Daños a datos computarizados: aquí se ubican los virus, las bombas lógicas, los gusanos, los accesos no autorizados, entre otros. Programas u acciones que de una u otra forma dañan la información de un sistema.
>
> Claves programáticas espías: conocidas como troyanos, o software espías, utilizadas para sustraer información en forma remota y física, preferiblemente aquella que le permita al delincuente validarse en el sistema bancario, suplantando a la víctima.
>
> Estafas a través de subastas en línea: se presentan en el servicio de venta de productos, generalmente ilícitos, en línea o en la red; se pueden encontrar celulares hurtados, software de aplicaciones ilegales, informáticos y entorno jurídico vigente en Colombia. Además, puede ser una vía de estafa ya que se suelen incumplir reglas de envió y de calidad de los productos solicitados.
>
> Divulgación indebida de contenidos: son conductas originadas en el anonimato ofrecido en el internet y el acceso público sin control desde ciber cafés; entre ellas se encuentran él envió de correos electrónicos anónimos, con fines injuriosos o calumnias, amenazas y extorsiones.
>
> Pornografía infantil en internet: a través de foros, chats, comunidades virtuales, transferencias de archivos, entre otras modalidades, los delincuentes comercializan material pornográfico que involucra menores de edad. Violación a los derechos de autor: utilizando reproductores en serie, los delincuentes realizan múltiples copias de obras musicales, video-gramas y software.

> Piratería en internet: implica la utilización de internet para vender o distribuir programas informáticos protegidos por las leyes de la propiedad intelectual. Aquí encontramos la utilización de tecnología par a par, correos electrónicos; grupos de noticias, chat y de internet, orden postal o sitios de subastas, protocolos de transferencia de archivos, etc. (Pág.2).

Una vez aclarado el concepto y las formas de ejecución de las conductas punitivas señaladas, es menester describir y realizar un análisis a fondo de la conducta más allá de las definiciones y modalidades del mismo, comprendiendo de este modo tanto la tipificación del delito como el modus operandi de quien los comete.

3.1.Descripción del delito

El profesor Julio Téllez Valdez, citado en el libro Delitos Informáticos del conferencista de legislación en delitos informáticos Luis Orlando Paloma, conceptualiza el delito informático como una conducta típica y atípica entendiendo a la segunda cuando se da el delito como fin, así mismo sostiene las siguientes características de dichas acciones delictivas citadas textualmente a continuación:

1. Solo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
2. Son conductas criminales del tipo “cuello blanco”: no de acuerdo con el interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete, dichos sujetos generalmente tienen posición social elevada por ende la motivación estos delitos no es por razones de inestabilidad económica, falta de conocimiento o inestabilidad emocional.
3. Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando
4. Son acciones de oportunidad porque se aprovecha de una ocasión creada por el atacante.
5. Provocan pérdidas económicas
6. Ofrecen posibilidades de tiempo y espacio

7. Presentan grandes dificultades para su comprobación, por su carácter técnico. (Paolma Parra, 2012).

3.2. Tipificación del delito

Para hablar de cualquier conducta entendida como delito la misma de contener sujetos, conducta, y un bien jurídico tutelado, además de que la misma sea antijurídica y culpable, de este modo si se hablara del sujeto activo del delito informático es el cibercriminal que sobrepasa la conducta descrita en la ley, en este caso es un sujeto indeterminado; la motivación de dicho delito no es de carácter exclusivamente económico o la búsqueda de causar una desmejora en el patrimonio moral y económico, sino que la misma corresponde a interés particulares demostrando destrezas del "depredador virtual". Con base en el análisis de estudios de las Naciones Unidas, en su manual para la prevención y control de delitos informáticos, el 90% de los delitos realizados a través de la computadora fueron ejecutados por empleados de la propia empresa afectada. De esta manera, nuevas exposiciones realizadas en América del Norte y Europa proporcionan significativas cifras: que el 80% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 20% corresponde a la actividad delictiva externa.

El sujeto pasivo seria las personas naturales o jurídicas que ven un menoscabo en sus intereses.

> No se debe perder de vista que de los sujetos sobre los cuales recae la conducta de la acción que realiza el sujeto activo, en el caso de los delitos informáticos que utilizan sistemas automatizados de información, habitualmente conectados a otros, el sujeto pasivo de la conducta es inmensamente significativo en estas agresiones virtuales, porque por razón de esas conductas alcanzamos a estar casi al tanto de los incomparables delitos cometidos por estos medios invisibles que es la potencia de la virtualidad que ejecutan estos cibercriminales. (Paolma Parra, 2012).

Bien jurídico protegido: La modificación del Código Penal señaló la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos dicho esto en el

Capítulo séptimo, son delitos pluriofensivos y de mera conducta. Este delito produce un doble daño el primero sobre el interés económico del particular y otro que recae sobre el interés estatal por la protección, defesa y salvaguardia del funcionamiento de los sistemas informáticos (datos e información).

3.3.Modus Operandi

En este tipo de delitos es difícil detectar la manera de actuar de los cibercriminales puesto que las acciones son hechas de forma fugaz y con sofisticación. El modo general de delinquir es a través de un hacker quien entra en los procedimientos técnicos para intentar o culminar el delito informático.

> un procedimiento bastante, usado en la banca en relación con este método es introducir una modificación al programa de tratamiento de cuentas corrientes para que siempre que se consulte el saldo de una determina cuenta lo multiplique por mil, por diez mil, o por cien mil, etc., con lo que es posible autorizar pagos, transferencia, por un importe muy superior al saldo real. (Márquez Cárdenas, 2009).

No obstante, el principal problema de este tipo de delitos es el desconocimiento real de quien los comete, impidiendo en cierto modo lograr probar su comisión, señala respecto a esto Meseguer Gonzalez (2013):

> ante la cantidad de técnicas de anonimato que el delincuente puede y suele usar, la prueba de los mismos se reduce a la exclusiva búsqueda y hallazgo de los rastros y pistas técnicas que ha podido dejar el ataque en el sistema usado para delinquir, lo que por un lado obliga a asegurarlos para evitar su pérdida o desaparición, y por otro a una continua y escalonada cadena intermedia de injerencias en derechos fundamentales ajenos (pág. 510).

Así las cosas, el delito informático, a pesar de ser una conducta penalmente reprochable, está ligado probatoriamente a la necesidad de un juez para su investigación, siendo por ende algo limitante y tortuoso la materialización de una condena para quien ejecuta la acción. Por tanto, tal y como lo señala Arocena Alonso & Esparza Liebar (2017):

> El tratamiento para los delitos informáticos no puede ser el mismo que se dispensa a los delitos clásicos o tradicionales. No se puede obviar el hecho de que la delincuencia informática tiene una serie de características intrínsecas que exigen un tratamiento procesal específico. (pág. 67).

4. Legislación Vigente

Con el aumento demográfico y con la masificación del acceso a internet dado en los últimos años se han podido identificar diferentes tipos de comisión de delitos informáticos en Colombia, los cuales son:

- Los que afectan el patrimonio económico: banca virtual, phishing, key logers, falsas páginas, venta a través de portales de compra y venta, falsos premios.

- Los que buscan el abuso de menores: comercializan videos, fotografía, audio, texto, falsas agencias, salas de chat.

- Los que afectan la propiedad intelectual: descargas de programas y comercialización de obras sin pagar derechos de autor.

- Los que afectan la información como bien jurídico:

> como por ejemplo cuando algunos empleados usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia, teniendo como base el desarrollo que han tenido. Robos de información privilegiada. (Manjarrez Bolaños & Jiménez Tarriba, 2012, pág. 77).

Teniendo en cuenta el incremento de las tecnologías novedosas que permiten la incursión en la red cibernética con gran facilidad, las leyes nacionales e internacionales han evidenciado una gran necesidad de fluctuar en beneficio del cubrimiento total de las posibilidades delictuales derivadas del consumismo tecnológico actual. De esta manera, las leyes colombianas han buscado fundamentalmente complementar el Código Penal creando un bien jurídico tutelado nuevo.

4.1.Análisis de la Legislación y Jurisprudencia Colombiana

Con el desarrollo jurídico logrado en pro de la protección de los datos que se encuentran en la red, Colombia se ha logrado ubicar al nivel de La Comunidad Económica Europea, quienes han ampliado los acuerdos relacionados con la protección de recursos informáticos de cada país, todo esto a través de La ley 1273 de 2009.

No obstante, dicha ley cuenta con diversos antecedentes que han, a su manera, tomado uno u otro delito que finalmente funcionaron como pilar para la concepción de los delitos informáticos. Para entrar en materia se mencionarán de forma sucinta las leyes y decretos que forjaron la conceptualización del bien jurídico tutelado creado por medio de la ley 1273 de 2009.

Inicialmente el Decreto 1360 de 1989: por medio de este se reglamenta lo relacionado con los derechos de autor frente a la creación de software, siendo entonces necesaria la inscripción de los mismo en el Registro Nacional de Derechos de Autor, resolviendo así las controversias generadas por las reclamaciones frente a la violación de dichos derechos. Señala Ojeda Perez J. E., Rincon Rodriguez, Arias Flores, & Daza Martinez (2010) que a partir de dicho decreto nació la legislación que busco

> Proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. (Pág. 52).

Continúa complementando la formación de un bien jurídico general que englobe los delitos informáticos la Ley 679 de 2000, en cuyo caso regulo la explotación de imágenes pornográficas y el turismos sexual de menores de edad, consagrando en su texto una prohibición clara a los proveedores o servidores, administradores o usuarios de internet o de las redes de comunicación global, de contener imágenes que de manera alguna implique la

explotación sexual o pornográfica de menores, haciendo de dicha conducta una sanción administrativa, mas no penal, es por tanto necesaria la expedición de la ley 1336 de 2009 que promulga la existencia de dos tipos penales relacionados con la materia a tratar, apoyando de esta manera la sanción interpuesta a través de la ley 679 de 2000.

Por otro lado, en el ámbito del derecho comercial y probatorio, se reconocen los medios electrónicos como eje fundamental el proceso, en primera medida la ley 527 de 1999 "ha reglamentado y definido el acceso y uso de los mensajes de datos, el comercio electrónico, la firma digital, el valor probatorio, la validez y eficacia de estos ante una acción judicial" (Muños Caro, 2016, pág. 13), mediante el Decreto 1747 de 2000 y es pos de complementar la ley anteriormente citada se determinan las condiciones o parámetros a cumplir por las entidades de certificación de la firma electrónica para efectos de su autorización, control y vigilancia en el mercado digital; finalmente pero no distante de lo aquí mencionando, la ley 794 de 2003 regula lo pertinente a las notificación por plataformas digitales, de modo que el avance en cuanto a desarrollo procesal con el fin agilizar el proceso ha sido notorio en los últimos años, lo cual implica la imperiosa necesidad de fortalecer los tipos penales que derivan de la comisión de conductas ilegales y arbitrarias dentro de los sistemas digitales

Al respecto señala Fernendez de Soto (2001):

> la cifra negra de la criminalidad, en materia de delitos informáticos, no puede seguir en la penumbra, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales la investigación de una nueva modalidad comisiva de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público.

En razón a esto el legislador utilizó los mecanismos necesarios para crear un conjunto de normas o leyes que propenden a la efectiva protección de la información creando "un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones". (Manjarrez Bolaños & Jiménez Tarriba, 2012, pág. 78).

A continuación se explicara un poco de la ley, para entender la regulación de estos derechos informáticos en el país, el primer Capítulo de la ley se divide en dos partes, la primera habla de la confidencialidad de la información, la integridad de los datos, la disponibilidad de los mismos y la segunda habla de los atentados informáticos

> A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos. (Manjarrez Bolaños & Jiménez Tarriba, 2012, pág. 78).

4.2. Desarrollo jurisprudencial y legal de algunos tipos penales de la ley 1273 de 2009:

Artículo 269A: Acceso abusivo a un sistema informático, este artículo inicialmente se sancionaba por medio de multa, razón por la cual se entendía una medida poco coercitiva extinguiendo la acción penal por medio de la ablación. Este precepto fue modificado con la entrada en vigencia de la ley 1273 de 2009 imponiendo una sanción mayor tanto cuantitativamente (pena) como pecuniariamente, posteriormente fue modificada por la ley 1288 de 2009, cambiando la sanción pero retornando al texto inicial, sin embargo la ley fue declara inexequible a través de la sentencia C-913 de 2010 con fundamento en que dicha ley debía ser expedida como estatutaria dado que la materia que desarrolla hace parte de elementos estructurales de los derecho de habeas data e intimidad. Así entonces el artículo 269A del código penal quedo establecido bajo los parámetros de la ley 1273 de 2009 que buscaba actualizar el ordenamiento penal colombiano frente a los atentados del sistema informático.

Articulo 269F: Violación de datos personales, con la creación del bien jurídico del título VII del código penal colombiano, el país tiene una regulación frente a los temas de protección de datos personales, diferente y complementaria a la Ley 1266 de 2008 que regulaba los aspectos

en el sistema financiero, de manera tal que, mediante la sentencia C-747 de 2011, se extiende la protección a todos los datos personales que se encuentren en os sistemas de computación.

Articulo 269I: Hurto por medio informáticos y semejantes: en este tipo el legislador trasladó los bienes jurídicamente tutelados por el hurto y sus circunstancias de agravación, entendiendo al mismo como uno de los actos de mayor peligro dado que las claves personales y empresariales son los únicos medios de defensa de los dineros depositados.

Por otro lado, la jurisprudencia colombiana ha avanzado a pasos agigantados frente al proceso de investigación de este tipo de delitos, dicho de este modo, Paolma Parra (2012) en su libro Delitos Electrónicos (en el ciberespacio) doctrina y análisis de casos reales señala:

> Las sentencias, entre otras, de la Corte Constitucional, la C-673 de 2005, sentencias que se conoce por que la Corte Constitucional indicó que el nombre del informante no se le puede ocultar al juez de garantías y por cuanto en la administración de justicia la verdad no se debe conseguir a cualquier precio; la C-336 de 2007 relativa a la búsqueda selectiva en base de datos, se refiere a lo imperativo de una orden judicial anterior o previa cuando se trata de obtener datos personales que se encuentran recogidos en establecimientos tanto públicos como privados y desde luego que tengan autorización legal para ello. En el mismo sentido se deberá acudir a la Ley 1266 de 2008, y en lo referente a la instrucción de la Corte Constitucional en sentencia C-747 de 2011; de igual forma es pertinente establecer la posible participación, ante el juez de control de garantías, posterior tanto a posible indicado como a su abogado una vez se haya celebrado audiencia de control de legalidad de esas diligencias, si así se pide; por ello la importancia de estas sentencias de la misma Corte, como la C-025 de 2009, entre otras. De la misma manera, es trascendental acudir a la Ley 527 de 2009, en donde aparecen definiciones tan importantes como los mensajes de datos, el comercio electrónico, firma digital, etcétera, para poder ingresar en la ley doce setenta y tres de dos mil nueve con mayor solvencia jurídica, y de esta manera realizar una adecuación típica escrupulosa. (pg. 182-183).

Permitiendo la estructuración del proceso para llegar a la imputación del indiciado sin posibilidad alguna de darse la violación al debido proceso y llegar a la culminación favorable del proceso.

Otro de los temas importantes a tratar frente a las nuevas tecnologías y el aporte de información a las mismas, es el derecho a la intimidad:

> que es pilar fundamental frente a la seguridad informática; tema que fue tratado, por la necesidad de hacer un análisis del conflicto, que se genera con el poder informático donde se expresa que la intimidad se protege para asegurar la paz y la tranquilidad (Montañez Parraga, 2017, pág. 40).

En razón a esto, la corte Constitucional ha establecido que en la medida en que avance la tecnología los derechos tales como el de información y el de intimidad se van limitado de acuerdo a las necesidades sociales y reales del momento.[1]

4.3.Legislación a nivel mundial para los delitos informáticos

Alemania: el primero de agosto de 1986, adoptaron la segunda ley en contra de una criminalidad económica contemplando delitos como: espionaje de datos, estafa informática, alteración de datos, etc. Este país condena delitos alejados de los contemplados en regulaciones afines, dado que no se castiga en intrusismo y la sagacidad ni sanciona el uso no autorizado de aparatos de procesos de datos

> En dicha legislación se desprenden cuatro posibles modalidades comisivas del delito: incorrecta configuración del programa, utilización de datos incorrectos e incompletos, utilización no autorizada de datos, cualquier otra forma de influencia no autorizada en el proceso de tratamiento de datos. El hecho punible, tiene que influir en el proceso de tratamiento de datos informáticos, esto significa que el autor influye de tal manera que se llega a cambiar el resultado de los datos almacenados en el computador, y el de aquellos que sean utilizados por el programa de trabajo. (Balmaceda Hoyos, 2009).

[1] Esto evidenciado en las Sentencias de la Corte Constitucional T 414/1992 [M.P. Ciro Angarita] y T 462/199 [M.P. Vladimiro Naranjo], en donde la corte asume una posición garantista de los derechos mencionados y detalla que “las tecnologías de la información nos está llevando a limitar cada día más la privacidad”

España: el código penal de España, castiga esta categoría de delitos aplicando pena de prisión, multa, con causales de agravación, cuando existe intensión dolosa o cuando se comente por un servidor público. En cuanto a estafas electrónicas, solo tipifica la misma cuando tiene ánimo de lucro y se realizan por medio de una manipulación informática sin detallar penas, siendo entonces este delito considerado como una estafa impropia, por el contrario, la legislación italiana en cuyo caso regula los delitos informáticos. En el artículo 640 del Código Penal Italiano se señala

> en el caso concreto una persona, antepuesta al control de la elaboración en un momento posterior al que intervino la manipulación, hubiera sido inducida en error a consecuencia de la intervención fraudulenta. Y justo sobre la base de consideraciones de este tenor, es que la jurisprudencia italiana ha aplicado a veces el art. 640, en el caso de manipulaciones de datos habientes a objeto de procesos informáticos que previeron todavía el concurso del hombre. (Balmaceda Hoyos, 2011, pág. 117).

Entonces, comprende la legislación italiana que el delito de estafa informática es similar o comparable con el delito de estafa tradicional, entendiendo que esta hipótesis es aplicable por cuanto el detrimento se ocasione a una persona propiamente dicha y no a un computador, ratificado así por Balmaceda Hoyos (2011) cuando

> para asegurar a la norma sobre la estafa informática un ámbito de operatividad circunscrito a las hipótesis en las que habría sido aplicable la norma de la estafa tradicional, si solamente la conducta fraudulenta se hubiera dirigido a una persona, en vez de a un computador. (pág. 117).

En cuanto a los avances legislativos de los países latinoamericanos en general frente al tema de los delitos cibernéticos, podemos evidenciar una serie de normas parciales que modifican los códigos penales de la mayoría de naciones, existiendo por esto diferencias sustanciales frente a los criterios penales necesarios para l configuración del tipo, teniendo en cuenta que los delitos informáticos no tienen límite de fronteras la no armonía entre legislaciones constituye un principal problema para el juzgamiento adecuado de dichos hechos delictivos, favoreciendo de cierto modo la ciberdelincuencia puesto que

> los países latinoamericanos han optado por diferentes posturas en relación con sus formas de regular. Algunos han optado por la sanción de leyes especiales, donde en los casos más destacados (caso de República Dominicana) incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso se han generado los organismos dedicados a su investigación y persecución. Otros tantos países (mayoría) han optado por modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos. (Temperini, 2014).

Así las cosas, se puede evidenciar una disparidad clara frente a la formación legislativa del derecho informático ante la comisión de los delitos cibernéticos tanto en el continente europeo como en el americano. Y en especial Latinoamérica, dejando entonces grandes vacíos de normatividad ante una situación delictiva de esta clase y por tanto mostrando en parte insuficiencia legal en los casos de aplicación normativa.

5. ¿Cómo afrontar la criminalidad económica?

De acuerdo con lo señalado a lo largo del presente artículo y en consideración con el desarrollo y vacíos normativos señalados en el acápite anterior y como concepto propio, se pueden consideran las siguientes opciones como alternativas suficientes para lograr dar frente a la criminalidad económica por vías tecnológicas:

1. Tomar medidas legislativas, es decir crear nuevos tipos para la clase de infracciones que surgen con el desarrollo de la tecnología, con la desmaterialización o des documentación de transacciones mercantiles solo basta con una operación electrónica para que se efectúen por lo cual se hace necesario estudiar las posibles conductas delictivas derivadas de las operaciones anteriormente descritas.
2. Implantar mecanismos elementales de seguridad. Es decir, buscar sistemas simples pero al mismo tiempo complejos, atendiendo a la capacidad humana de memorizar cierta cantidad de números clave, incluyendo también la amplia gama de comercio de dispositivos de seguridad que pueden ser útiles para la enseñanza de cuidados y seguridad en la red.

3. Instruir y formar grupos policiales para perseguir este tipo de delitos, entendiendo que la instrucción requiere personal capacitado para que, una vez teniendo éxito, se pueda dar la prevención e investigación de figuras criminales con conocimientos complejos, no solo de carácter informático, sino mercantil, financiero y empresarial que están sujetos a la posibilidad de ser objeto del daño (Márquez Cárdenas, 2009).
4. Buscar la homogenización legislativa a lo largo de los países latinoamericanos, con el fin de evitar la generación de paraísos delictivos por blandas sanciones frente a los delitos cibernéticos o por imposibilidad de comparar las sanciones y metodologías de investigación entre un país y otro.

5.1. Critica a la eficacia de la legislación e instituciones estatales para la prevención del delito

A lo largo del texto de este artículo se han venido estableciendo una serie de normas y conductas reprochables dentro del ámbito delictual comprendido por el avance tecnológico de la realidad cambiante y actual del mundo, dichos cambios entendidos como el uso indeterminado de internet, el acceso y manejo constante y fluctuante de información que a la luz de la normatividad nacional no haya control total o efectivo para la identificación verídica de la persona natural o jurídica encargada de dichas actividades delictivas, asumiendo la política de neutralidad en la red, estableciendo el derecho a la privacidad de los usuarios cibernéticos.

Así las cosas, en Colombia puntualmente hablando en razón al derecho a la privacidad y a la neutralidad de la red ha creado por así decirlo un bien jurídico tutelado para quienes actúan como victimarios, haciendo complicada la investigación y juzgamiento por parte de las instituciones encargadas de ello y por tanto entrando en una flexibilidad latente que implica el evidente atraso legislativo frente a la realidad socio-cultural del avance de la tecnología y de las operaciones comerciales que en razón a este se generan. Señala Quintero Porras (2016) que Colombia

> siguiendo directrices internacionales como las emanadas en Convención de Palermo, avance hacia un tratamiento penológico de las personas jurídicas, con base en lo que

> se considera, es la ausencia de responsabilidades severas que hacen que se usen las organizaciones para la acción delictiva. (pág. 29).

En razón a esto, cabe resaltar la necesidad de fortalecer las acciones jurídicas institucionales adelantadas por el estado colombiano, con ocasión de los delitos informáticos, teniendo en cuenta que las medidas actuales son endebles e insuficientes en comparación con la capacidad e ingenio de quienes incurren en dichas conductas.

Conclusiones

Las tecnologías informáticas están en constante cambio, el avance tecnológico mundial, hace difícil el acaparamiento de todas las situaciones delictivas que surgen a partir de la misma; lo que hace menester la inclusión del Estado en el desarrollo de inteligencia ante los casos posibles de conductas encaminadas al daño como método, fin, o medio de los delitos informáticos.

Es por esto que el avance legislativo del tema aunque se ha desarrollado de forma macro, más encaminada al proceso, siguen existiendo vacíos jurídicos frente a los temas de carácter microscópicos, como los delitos informáticos con aval de servidores públicos o los cometidos con anterioridad a la legislación.

Es allí donde surge la necesidad no de crear nuevos tipos sino de clarificar y llenar los tipos existentes, crear un grupo especializado no solo en materia de delitos informáticos, sino en información financiera, bancaria y mercantil para dar mayor confiabilidad a la investigación y finalmente crear conciencia en la población de la existencia de este tipo de delitos, en modalidades de operación, por medio de campañas educativas que enmarquen verdaderamente lo que se refiere a delitos de carácter informático

En el marco internacional de la región es importante fortalecer la igualdad de sanciones criterios para las mismas, considerando que

> La delincuencia informática, como conjunto de los varios crímenes que se denotan por la presencia de alguna tecnología, es un fenómeno global, como es global la red, y por lo tanto, si se quiere limitarlo, la coordinación a nivel internacional es una necesidad imprescindible. (Gamba, 2010, pág. 22).

Finalmente, podemos concluir en el presente trabajo que con el descubrimiento en Colombia del Caso Soto Prieto, como precursor y ejemplo de la comisión de delitos electrónicos que implican la defraudación de la confianza y el aprovechamiento de las redes con el fin de apropiarse o por demás vulnerar bienes jurídicos tutelados ajenos, se abrió la puerta para el reconocimiento del avance tecnológico como fuente de conductas fácilmente ilegales y que, en un principio, bajo una regulación macro, como la existente en la actualidad, debe ser cubierta; sin embargo el constante cambio tecnológico requiere de la actualización de los códigos que regulan las sanciones y por ende la limitación de los derechos y deberes de las partes consumidoras de las redes globales, así mismo la creación de leyes específicas e instituciones capacitadas para la investigación y reconocimientos de los delitos señalados.

BIBLIOGRAFÍA

Arocena Alonso, L., y Esparza Liebar, I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. Novum Jus, 11(1), 39-72.

Avendaño, D. (2017). Sistema Informático, confidencialidad, integridad y disponibilidad de datos en la red. Revista de delitos informáticos, 1-23.

Balmaceda Hoyos, G. (2009). El delito de Estafa Informática. Bogotá: Leyer.

Balmaceda Hoyos, G. (2011). El delito de estafa Informática en el derecho europeo continental. Revista de derecho y ciencia penales, 111-149.

Bolívar Mesa, M. A. (2018). Las medidas cautelares innominadas y su relación con el principio de legalidad. (Trabajo de Grado) Bogotá: Universidad Católica de Colombia.

Cáceres Corrales, P. J. (2013). Las formas cambiantes de la criminalidad, Colombia a finales del siglo XX. Bogotá: Universidad Nacional de Colombia.

Computer Forensic. (s.f.). www.delitosinformaticos.info, delitos informáticos. Recuperado el 23 de Septiembre de 2019, de Definición de Delio Informático: https://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Budapest.

El Tiempo. (6 de Abril de 1984). ¿Quiénes son los responsables? El tiempo, pág. 8A.

Fernández de Soto, M. C. (2001). Atipicidad relativa en los delitos de la falsedad, hurto, estafa y daño informáticos. Bogotá: Universidad Sergio Arboleda.

Gamba, J. (2010). Panorama del derecho informático en américa latina y el caribe. Santiago de Chile: Comisión económica para América Latina y el caribe (CEPAL)

García Vásquez, J. C. (23 de Julio de 2012). Genealogía Colombiana Volumen II. Obtenido de Interconexión Colombia: http://www.interconexioncolombia.com/documentos/genealogia/tomo2/1.33.%20LA%20LISTA%20DEL%20PENTAGONO-CEBOLLERO-EDUARDO%20Y%20PAULINA%20ZULETA%20JARAMILLO-ROBERTO%20SOTO%20PRIETO-ALVARO%20Y%20JORGE%20%20LEIVA.pdf

Hillon Vega, J. T. (2000). El Estado de las Cosas o la increíble y triste historia de la convención interamericana contra la corrupción. Bogotá: Pontificia Universidad Javeriana.

Holguín, C. (1991). El fraude de los US$13.5 millones. Proceso de la Republica de Colombia ante la corte de Londres. Bogotá: Banco de la Republica.

Lima, M. l. (1984). Delitos Electrónicos. México: Porrúa.

Loredo González, J. A., y Ramírez Granados, R. (2013). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Nuevo Leo, México: Universidad Autónoma de Nuevo León.

Manjarrez Bolaños, I., y Jiménez Tarriba, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82.

Marquez Cárdenas, A. E. (2009). La delincuencia económica. Bogotá: Ediciones Doctrina y Ley LTDA.

Meseguer González, J. D. (2013). Los nuevos Modi Operandi de los Ciberdelincuentes durante la crisis económica. Revista de Derecho UNED, 495-523.

Montañez Parraga, A. C. (2017). Análisis de los delitos informáticos en el actual sistema penal colombiano. Bogotá: Universidad Libre de Colombia-

Muños Caro, L. F. (2016). Del derecho electrónico en Colombia: interpretación normativa, producción y valoración probatoria de la firma digital y/o electrónica (Trabajo de Grado). Bogotá: Universidad Católica de Colombia.

Ojeda Perez, J. E., Rincón Rodríguez, F., Arias Flores, M. E., y Daza Martínez, L. A. (2010). Delitos Informáticos y Entorno Jurídico Vigente en Colombia. Cuadernos de Contabilidad, 41-66.

Paloma Parra, L. O. (2012). Delitos Informáticos (en el ciberespacio): doctrina y análisis de casos reales. Bogotá: Ediciones Jurídicas Andres Morales.

Quintero Porras, C. O. (2016). La acción delictiva a través de la informática en Colombia: el caso particular de lavado de activos y la lucha institucional contra su configuración. (Trabajo de Grado) Bogotá: Universidad Católica de Colombia.

Rinaldi, P. (27 de Abril de 2017). ¿De dónde viene el delito cibernético? origen y evolución del delito cibernético. Obtenido de Le VPN: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Rodríguez Arbeláez, J. D. (2011). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Recuperado el 10 de octubre de 2019, de http://bdigital.ces.edu.co: http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

Temperini, M. I. (2014). Delitos Informáticos en Latinoamérica: un estudio de derecho comparado. Buenos Aires: Simposio Argentino de informática y derecho.

Torres Estepa, A., López Sanabria, I. F., y Sarmiento Avella, M. A. (s.f.). "IN" Seguridad de la información y delitos informáticos en Colombia. Bucaramanga: Universidad Autónoma de Bucaramanga.

Torres Torres, H. W. (2002). Derecho Informático. Medellín: Ediciones Jurídicas.

Sentencias

Corte Constitucional, Sala Plena. (30 de junio 2005) Sentencia C-673 /2005 [M.P. Clara Inés Vargas Hernandez]

Corte Constitucional, Sala Plena. (9 de mayo 2007) Sentencia C-336 /2007 [M.P. Jaime Córdoba Triviño]

Corte Constitucional, Sala Plena. (5 de octubre de 2011) Sentencia C-747 /2011 [M.P. Nilson Pinilla Pinilla]

Corte Constitucional, Sala Plena. (27 de enero 2009) Sentencia C-025 /2009 [M.P. Rodrigo Escobar Gil]

Leyes y Decretos

Congreso de Colombia. Ley 599 de 2000, Código Penal Colombiano. Diario oficial número 44.097 del 24 de julio de 2000

Congreso de Colombia. Ley 1273/2009. Diario oficial número 47.223 del 5 de enero de 2009.